STATE OF MONTANA
DEPARTMENT OF CORRECTIONS
POLICY DIRECTIVE

Policy No. DOC 1.7.7	Subject: **COMPUTER SECURITY**	
Chapter 1: ADMINISTRATION AND MANAGEMENT		Page 1 of 3 and Attachment
Section 7: Information Systems		Effective Date: Dec. 1, 1996
Signature: /s/ Mike Ferriter, Director		Revised: 07/26/11

I. POLICY

The Department of Corrections administers computer security to prevent the intentional or unintentional modification, destruction, disclosure, or misuse of data and information technology resources, and to remain in compliance with state laws and policy.

II. APPLICABILITY

All divisions, facilities, or programs Department-owned or contracted, as specified in contract.

III. DEFINITIONS

Data and Information Technology Resources – The State mainframe computer; the State’s and the Department's mid-range computers and file servers; the Internet and intranet; Local, Wireless, Virtual and Wide Area Networks (LANs,VLANS, WLANs & WANs) and associated equipment; microcomputer hardware and software, printers and other peripherals; facility resources related to computing, electronically stored data, email services, and other related resources.

Password – An alphanumeric combination of characters unique to individual users that allows access to a specific computer, network or computer system.

User ID – Used generically to refer to CI number, login ID, ACF2 ID, user account, or any other term used to describe a user's unique identifier which is used to grant rights and privileges on a computer, computer system or network. User IDs are never reused.

IV. DEPARTMENT DIRECTIVES

A. General

1. The Department has delegated its statutory authority for the security of data and information technology resources to the Information Technology (IT) Division.

2. The IT Division will appoint a security officer(s) to handle daily activities related to providing staff access to the systems and data needed to perform their jobs.

3. Department data, in general, belongs to the Department’s programs; the IT Division functions as the "caretaker" of data for programs by granting and restricting access on behalf of the owners of each set of data.

4. Each facility/program/division will appoint a security coordinator to work with the IT Division; the security coordinator will receive requests from local staff for new or changed access to systems and data and, when approved, forward them to the IT Division

security officer through the IT Service Desk for implementation. The program that "owns" the data must approve access requests from another program before access is granted.

5. The security officer may develop and implement additional procedures to protect the integrity of, and access to, Department data and information technology resources.

6. The IT Division grants data access on a "most restrictive" or "least rights" basis; users are granted the lowest level of access possible to accomplish their job functions.

7. Local security coordinators will notify the security officer via the IT Service Desk whenever an employee changes positions within the Department and request appropriate changes to the employee's access rights. Security coordinators will also notify the IT Service Desk when an employee discontinues employment or is terminated so access to systems and data may be adjusted.

B. User ID and Passwords

1. Each employee allowed access to any Department information system will be assigned a User ID and password; applications that run on these systems may require a separate User ID and password. By accessing Department IT resources, the employee is agreeing to follow Department policy.

2. User IDs and passwords grant individual rights that vary depending upon job requirements; i.e., employee "A" may have a User ID that allows access to all parts of the Offender Management Information System (OMIS) while employee "B" has a User ID that grants access to only certain parts of OMIS.

3. Employees must protect the confidentiality of their User ID and password, may not share the information, and may not write the information where others could find them.

4. Employees will not remain signed onto systems when absent from the computer or terminal for fifteen minutes or longer and, unless otherwise directed, will power off their computer when leaving the work area at the end of their workday.

5. If employees violate this policy, computer rights will be immediately terminated. Supervisors may not reinstate individual computer rights before assuring the security officer that steps have been taken to prevent further violations.

6. The IT Division may grant emergency access to an absent employee's data and/or email account if approved by the appropriate supervisor from the program "owning" the data; requests will be made in writing with a limited time frame and be evaluated on a case-by-case basis by the security officer.

V. CLOSING

Questions concerning this policy should be directed to the Department's Chief Information Officer (CIO).

VI. REFERENCES

A. 2-15-112, MCA; 2-15-114, MCA; 2-17-534, MCA
B. 1-0250.00 Montana Operations Manual
C. ENT-SEC-063, ENT-SEC-072; Enterprise IT Policy
D. DOC Policies 1.7.3, Data Quality; 1.7.6, Unlawful Use of Computers; 1.7.9, Acceptable Use of IT Resources

VII. ATTACHMENT

IT Consent PDF